

**Policy and Evaluation Division**

**Information Security Unit**

**Audit of  
Prison Industry Authority  
DIGITAL SERVICES**

**Institution Name**

**(Date)**

## TABLE OF CONTENTS

Introduction		
Scope and Methodology		
Executive Summary		
Explanation of Findings		
Chart of Findings		
Statistical Summary		
Audit Criteria and Findings		
	Section A – Physical Security	
	Section B – Network Security	
	Section C – Data Management	
	Section D – Program Management	
Glossary		
Corrective Action Plan		
Attachments		
	Attachment A – DSE Security Plan	
	Attachment B – Department Operations Manual, Sections Cited	

## **INTRODUCTION**

This audit of the PIA Digital Services Program at Mule Creek State Prison (MCSP) was conducted Policy and Evaluation Division, with the assistance of PIA staff on (date).

The audit consisted of on-site inspection, interviews with staff, reviews of procedures and other documentation.

The purpose of this audit is one of overall analysis and evaluation of the PIA's compliance with the terms and conditions of applicable State regulations, DOM and information security standards.

## **AUDIT SCOPE AND METHODOLOGY**

The purpose of this audit is to assess the level of compliance with established policy and regulations and the Security Plan for the Digital Services Program.

The scope and methodology of this audit are based on written audit procedures developed by the Policy and Evaluation Division and provided to Mule Creek State Prison (MCSP) staff in advance of the audit. The audit consists of two phases:

**Evaluation.** PED staff, using the audit finding areas as a guide, evaluate the operation of the Digital Services Program and determine the compliance in each of the finding areas.

**Findings Resolution Action Plan.** The PED staff work with Digital Services staff and PIA Headquarters to identify reasonable means by which findings identified during the Evaluation Phase of the audit can be resolved.

This audit is completed with the delivery of the report of findings and associated action plan.

For the purpose of this audit, the auditors toured the PIA facilities at Mule Creek State Prison (MCSP). Utilizing "point-in-time" methodology, information was evaluated against all administrative requirements.

## **EXECUTIVE SUMMARY**

During this audit of compliance with State regulations and CDC/PIA-established Digital Services Security Plan, the facility was found to be in partial compliance with an overall score of XX%.

Issues were found in the following areas:

## **EXPLANATION OF FINDINGS**

The following chart represents individual audit findings.

Each of the items are rated as to whether or not the institution is in compliance. The chart utilizes the following symbols to denote compliance ratings:

<b>RATING</b>	<b>DEFINITION</b>
<b>Compliant (C)</b>	The requirement is being met.
<b>Partially Compliant (PC)</b>	The institution is clearly attempting to meet the requirement, but significant discrepancies exist.
<b>Not Compliant (NC)</b>	The institution is clearly not meeting the requirement.
<b>Not Rated (NR)</b>	No measurable instances.

At the end of the chart is a Statistical Summary of Audit Findings. This summary presents a mathematical breakdown of compliance by total items and percentages (%).

**Prison Industry Authority**  
**Digital Services Enterprise**  
**At**  
**Mule Creek State Prison**

**CHART OF FINDINGS**

AUDIT STANDARD		AUDIT FINDING Feb 2003	Page
<b>A PHYSICAL SECURITY</b>			
1	All DSE computers have appropriate signage		1
2	Inmate work areas marked and observable by staff		1
3	Access to DSE facilities limited to authorized persons		1
4	Outside communications in inmate work areas		1
5	Access to server and annex rooms off limits to inmates		1
6	Asset Control		
	a. Inventory Maintained		1
	b. Inventory is accurate and current		1
	c. Adherence to Software Licensing		1
	d. Information Technology acquisitions conducted appropriately		1
	e. CABS directories removed from and inaccessible to inmate computers		1
	f. Proscribed commands removed from inmate computers		1
	g. Inmate access to scanners controlled by supervisors		1
	h. Inmate access to output devices controlled by supervisors		1
<b>B NETWORK SECURITY</b>			
	Network Administration		
7	Network Documentation		2
8	System configuration logs		2
9	Internet access log		2
10	Dialup access		
	a. Modems located in the server room or inmate work area?		2
	b. RAS enabled?		2
11	Firewall documentation		
	a. Access Control Lists		2
	b. Firewall Rules		2
	c. Ports and Services		2
12	Malicious Code Protection		

	a. virus protection software kept current		2
	b. When was the DAT file last updated?		2
	c. How is the DAT file propagated to all systems		2
	d. Schedule for scanning servers		2
	e. Schedule for scanning workstations		3
	Inmate use of the DSE Network		
13	Inmates have Administrator Privileges		3
14	Inmates' profile restricted		3
15	Inmates' access to workstations limited to single assigned machine		3
16	Inmate computer disks and floppies audited regularly		3
17	Staff using the same computer for non-DSE purposes?		3
18	Inmates' access to confidential information		3
	Account Administration and Access Authorization		
19	General		
	a. Old and obsolete user IDs deleted		3
	b. Old and obsolete visitor and guest IDs		3
	c. Responsibility for FTP account activity		3
	d. Unnecessary FTP accounts removed		3
	e. Screensavers on workstations set to five minute activation		3
	f. All users have unique user IDs		3
20	Staff user IDs and passwords		
	a. All staff received annual information security awareness training		3
	b. User agreement forms current		4
	c. Password integrity		4
21	Inmate User IDs and Passwords		
	a. All inmates cleared for computer use		4
	b. Management of passwords for inmate accounts		4
<b>C DATA MANAGEMENT</b>			
22	Incoming Data		
	a. All data inspected and personal and confidential info removed		5
	b. Electronic files delivered to DSE in accordance with Security Plan		5
	c. All data labeled as such for inmate access		5
23	Outgoing data		
	a. All data inspected for unauthorized content		5
	b. Data transferred out of DSE in accordance with DSE Security Plan		5
	c. Who inspects the data?		5
24	Data management on the DSE system		
	a. Backup schedule for servers		5
	b. Backup storage		5
	c. Testing of the backup processing		5



<b>D PROGRAM MANAGEMENT</b>			
25	Security Committee quarterly meetings Security Plan update Security Committee members Information Security Coordinator for the DSE		6
26			6
27			6
28			6

**Prison Industry Authority  
Digital Services Enterprise  
At  
Mule Creek State Prison  
STATISTICAL SUMMARY**

## I. Audit Criteria and Findings





### SECTION A – PHYSICAL SECURITY

This section of the audit pertains to the physical security of the DSE facilities, including inmate and staff work areas, server room, computer and network asset management, and accessibility of network resources such as printers, scanners and plotters. Following are the policy sections supporting the finding areas:

1. Are all computers clearly marked with appropriate signage? (DOM Sec 42020.6)
2. Are inmate work areas clearly marked as such and located in such a manner that staff may observe them? (DOM Sec 42020.6)
3. Is access to the DSE facilities limited to those authorized? (SP 2.3.2)
4. Are there any outside communications devices (phones, faxes, modems or other network devices that enable connectivity) located in areas where inmates work? (DOM Sec 42020.6)
5. Is access limited to all areas where servers and network components are located? This would include but not be limited to the Annex and Server Rooms. Please provide annex inspection log for review. (SP 2.3.1; 2.3.3; 2.3.4; 4.1.1)
6. Asset Control
  - a. Is an inventory of information technology assets maintained? (DOM 46030.1)
  - b. Is the inventory accurate and current, including software, peripherals, assigned user(s) and physical location of each system? (DOM 46030.4)
  - c. How does PIA insure adherence to software laws? (SP 5.1; DOM 48010.10.1)
  - d. Are Information Technology acquisitions conducted appropriately?
  - e. Are CABS directories removed from inmate computers? Can an inmate logon provide access to these directories on another computer on the network?
  - f. Are the proscribed commands (DEBUG, ASSIGN & ATTRIB) removed from all inmate-access computers? (DOM 49020.19)
  - g. Is access to scanners controlled by supervisors? (SP 2.3.2)
  - h. Do inmates have access to output devices eg. printers or plotters? (SP 2.3.2)

## SECTION B – NETWORK SECURITY

### Network Administration

7. **Provide the most current network documentation. This should include the system configuration diagram, and a complete list of all systems, including their IP addresses, assigned user(s), network identification, and physical location. (SP3.1)**
8. **Provide the system configuration log showing when each software patch and other installation was made, and by whom.**
9. **Provide the log of internet access made from any node on the network, including all access through the firewall.**
10. **Dialup access (SP 3.2.1)**
  - a.  **Are there modems either in the server rooms or in the inmate work area?(SP 3.2.1;DOM 49020.19.5)**
  - b.  **Is RAS (Remote Access Server) enabled? (SP 3.2.1)**
11. **Provide firewall documentation. This includes:**
  - a. **Access Control Lists (ACLs). The ACLs should correspond to the list of authorized users allowed access through the firewall.**
  - b. **Firewall Rules. The Rules should provide filters to block all unauthorized incoming traffic, all known spoofing techniques, common DoS strategies.**
  - c. **Ports and Services. A port scanner should be run to identify all open ports and  services on the network. This should be compared to the services and ports authorized, and any discrepancies noted as findings.**
12. **Malicious Code Protection:**
  - a. **What is the process by which the virus software is kept current? This should be an automated service that requires no intervention from PIA staff.**
  - b. **When was the DAT file last updated? The DAT file found on the system should correspond to the most current available on from the virus software provider.**
  - c. **How is the current DAT file propagated to all network servers and workstations?  This should be an automated process requiring no intervention. It should be scheduled to occur at least once weekly.**
  - d. **How often are servers scanned for viruses. This should be daily.**

- e. **How often are workstations scanned. This should be no less than weekly.**


### **Inmate Use of the DSE Network**

- 13. **Do inmates have Administrator privileges? (SP sec 2.1.3; 3.3.2)**
- 14. **Are inmate user profiles restricted to “as needed for function only”? (SP sec 2.1.4)**
- 15. **Are inmates limited in access to a single workstation on the network? (SP 3.3; s.4.7)**
- 15. **Do inmates have access to systems outside of the DSE, email, shared folders or other network-enabled communications? (SP 2.1; 3.3.2)**
- 16. **Are inmate hard drives and floppy diskettes checked for data integrity and/or misuse on a regular basis? (SP Sec 2.2.1; 3.2.2)**
- 17. **Are staff using the same network for purposes other than those required to monitor inmate activity and other system administration purposes? (DOM Sec. 42020.6 and 48010.9; SP 2.3.2)**
- 18. **Do inmates have access to confidential, sensitive or personal information? (SP 2.3.1)**

### **Administration of User Accounts, Passwords and Access Authorization**

**At the time of the audit there are \_\_\_\_ assigned staff in the DSE and \_\_\_\_ assigned inmates.**

#### **19. General**

- a. **Are there old or obsolete user IDs on the system?**
- b. **Are there obsolete or old a “visitor” or guest logons? (SP 3.3.3)**
- c. **Who is responsible for File Transfer Protocol Accounts? (SP 3.3.4)**
- d. **Have all old FTP accounts been removed? (SP 3.3.4)**
- e. **Are all accounts configured to utilize the screensaver password feature set to  minutes activation? (SP 3.3)**
- f. **Does every user on the system, including staff, inmates and limited access accounts, have a unique user ID and password? (SP 3.3)**

#### **20. Staff User IDs and passwords**

- a. **Have all staff received information security awareness training in the last twelve months? (DOM 49020.17)**

- b. Are user agreement forms current (DOM 49020.9.1; 49020.4)**
  - c. What measures are taken to protect passwords from compromise? (DOM 49020.9.2)**
- 21. Inmate User IDs and Passwords**
  - a. Have all inmates been cleared for computer use through the MCSP Inmate Work Assignments process? (SP 1.1)**
  - b. How are passwords managed for inmates? (SP 3.3.2)**



## **SECTION C - DATA MANAGEMENT**

### **22. Incoming Data**

- a. Are all data, including hard copy and electronic files, inspected and cleaned of personal and confidential data prior to inmates' access? (SP4.1.1)**
- b. Are incoming electronic files delivered to the DSE facility in accordance with the DSE Security Plan? (SP 4.1.2)**
- c. Are all data clearly labeled as being ready for inmate access? (SP4.1.3)**

### **23. Outgoing Data**

- a. Are all data ready for transfer out of DSE inspected to ensure no unauthorized content, in accordance with the DSE Security Plan?**
- b. Are the processes described in the Security Plan followed when data are transferred using the network? (SP 4.2)**
- c. Who inspects data? (SP4.2)**

### **24. Data Management While on the DSE System**

- a. How often are the servers backed up? (SP 6.2.3)**
- b. Where are the backups stored? (SP 6.2.3)**
- c. When was the last time the recovery from backup process was tested? (SP 6.2.3)**

## **SECTION D - PROGRAM MANAGEMENT**

- 25. The DSE Security plan stipulates that the Security Committee meet quarterly. When was the last time the Committee met? (SP 7.2)**
- 26. The Security Plan requires that the Plan be reviewed, updated as required and approved by the Committee annually. When was the last time the SP was updated, reviewed and approved? (SP 7.1)**
- 27. The Security Plan requires that staff from the PIA, MCSP Information Services and the CDC Information Security Officer serve as member of the DSE Security Policy Committee. Who are the current members sitting on this committee? (SP 7.2)**
- 28. Has a PIA employee been designated the Information Security Coordinator for this program? (DOM 49020.11; SP 3.3)**



## Glossary

<b>AISA</b>	Associate Information Systems Analyst
<b>CABS</b>	Cabinet files (electronic)
<b>CCR</b>	California Code of Regulations
<b>CD</b>	Compact Diskette
<b>CDC</b>	California Department of Corrections
<b>CDC Form 1855</b>	Workgroup Computing Justification Form
<b>DOM</b>	Department Operations Manual
<b>DOS</b>	Disk Operating System
<b>FRAD</b>	Frame Relay Access Device
<b>ICS</b>	Inventory Control Sheet
<b>ID</b>	Identification
<b>ISB</b>	Information Security Branch (Department of Corrections)
<b>ISC</b>	Information Security Coordinator
<b>ISD</b>	Information Systems Division (Prison Industry Authority)
<b>ISO</b>	Information Security Officer
<b>ISU</b>	Information Security Unit
<b>LAN</b>	Local Area Network
<b>MAPS</b>	Manufacturing and Accounting Planning System
<b>NOS</b>	Network Operating System
<b>OOC</b>	Office of Compliance
<b>(PC)</b>	Penal Code
<b>PC</b>	Personal Computer
<b>PFAB</b>	Program and Fiscal Audits Branch
<b>PIA</b>	Prison Industry Authority
<b>(SP)</b>	Security Plan
<b>TCP/IP</b>	Transfer Control Protocol/Internet Protocol

## **Corrective Action Plan**

## **CDC Department Operations Manual, sections cited in Audit Findings**

### **Dom 42020.6 Inmate Access to Computers**

All facilities with inmates accessing computers in any capacity, including inmate education programs, shall comply with the following procedures:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Areas where inmates are authorized to work on computers shall be posted as such.
- There shall be no communication capabilities such as telephone, computer line, or radio communication devices in the area.
- Inmates shall not have access to utility programs such as Mace, Norton Utilities, or PC Tools.
- Inmates shall not have access to the MS-DOS commands DEBUG, ASSIGN, and ATTRIB.

### **46030.1 Policy**

The Department shall maintain an accurate inventory of its EDP equipment, peripheral devices, and software. All purchased EDP equipment shall concur with the technical specifications contained in the SAM 5005. All EDP hardware shall be inventoried at the time of installation, identified with a CDC property tag, and if site requirements necessitate, permanently marked by engraving with the CDC property tag number, item serial number, and DGS billing code number

### **46030.4 Documentation for Inventory of EDP Equipment**

The EDP inventory shall include the following data elements:

- Primary Location: division/branch, facility, or parole region where equipment is located.
- Secondary Location: unit or office where equipment is located.
- Brand of Equipment: monitors, keyboards, printers, etc.
- Model Number: monitors, keyboards, printers, etc.
- Serial Number: monitors, keyboards, printers, software, etc.
- Ownership: whether CDC or specified other owns
- Version Number: software.
- Date of Acquisition: date equipment was received.
- Date of Installation: date equipment/software was installed.
- Date of Relocation: date equipment/software was relocated.
- Relocation Location: unit or office where equipment has been relocated.
- Signature: signature of local AISA or designee or AISA's supervisor.

#### **48010.10.1 Copyright Material and Licenses**

Software license agreements shall be strictly adhered to. Proprietary software cannot be duplicated, modified, or used on more than one machine, except as expressly provided for in the manufacturer's license agreement program updates may be downloaded from the Internet in accordance with the owner's license agreement.

Public domain software, while available under the copyright laws to all individuals should not be downloaded to a departmental workgroup computing device unless it is part of the departmental standard as documented by the Workgroup Computing Coordinator and/or approved by the unit manager.

#### **49020.4 Responsibility**

The access management group and each organization with owner or custodial responsibilities for an information system have the following access management responsibilities:

- Access Authorization. The granting of permission to execute a set of operations in the system. At the lowest level, for example, this would be to grant permission for inmate trust personnel to access the classification of inmates on the DDPS. At the highest level, for example, this would be working with the information system owners to physically allow access to a specific information system.
- Access Control. Enabling the performance of tasks by hardware, software, and administrative controls that would have the effect of monitoring a system's operation, ensuring data integrity, performing user identification, recording system access and charges, and granting access to users.
- Accountability. The work necessary to set up the ability to trace violations or attempted violations of system security to the individual(s) responsible.

#### **49020.9.2 Information Security- Responsibilities of Password Owners**

*Revised April 16, 1993*

Access to CDC's dedicated computers is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. Authorized persons engaging in a terminal session with a computer shall log off (terminate the session) before leaving the immediate vicinity of the terminal, because the password which allowed the session to begin remains in effect throughout the session. Additionally, no ability shall exist for a user to store, load, or invoke the log on process, on any CDC computer, by any method that includes the user Resource Access Control Facility (RACF) ID or the password. Violation of this policy may result in the revocation of all access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those having used the password.

The password is a major "key" to the integrity of CDC's automated environment. This policy exists to protect the integrity of that key.

User IDs shall never be shared. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what the password is.
- Not write down the password.
- Not use an obvious password. Obvious passwords include one's name or nickname, the names of one's children, one's user ID, names or words associated with hobbies ("DANCER," "SKI BUM," etc.), names associated with favorite books or movies ("JEDI," "LUCAS," "SCARLET," "RHETT," etc.), "SECRET," "SECURE," "PASSWORD," car or

driver's license numbers, the name of the current month, etc. Non-obvious passwords use foreign languages (e.g., Latin), word combinations rather than single words, random combinations of letters and numbers, etc.

- Not leave an active terminal session.

If the password owner becomes aware that a correct password is being rejected, that user should immediately notify the local ISC, the AMG, and the ISO, since this may indicate that someone has discovered the password and has changed it without the owner's permission, resulting in the owner no longer knowing his or her own password.

If a password is forgotten, the local security coordinator or the AMG shall be telephoned. They shall validate the owner's identity and give a new temporary, one-time password. The owner shall change this password immediately.

If anyone asks for a password, the owner shall refuse to provide it and shall refer the person to a supervisor. The owner shall then notify the supervisor.

Anyone who knows that any password has been compromised should take the following actions:

- Notify the ISC.
- Notify the ISO.
- Complete a "security incident report." For further information on this document, see the reports section of this policy.

#### **49020.9.3 Information Security- Responsibility of Employers of Password Owners**

*Revised April 16, 1993*

People are provided passwords because their jobs require them to access CDC ITS. Therefore, whenever a password owner terminates employment or is reassigned to duties that do not require such access, the immediate supervisor shall, without delay, notify the applicable party of the change.

The authority to access CDC computers entails a significant risk to the Department's ability to function. Therefore, such authority is restricted to persons with a demonstrated need for access. Because that need is, by definition, a function of the person's specific job duties, any change in those duties requires a reevaluation of the need for access. If the duties change such that the need for access no longer exists, the access shall be revoked.

If any password owner changes job duties (by resignation, promotion, transfer, reorganization, separation, etc.), that individual's immediate supervisor shall refer to the security organization chart (distributed separately) for appropriate contact names and telephone numbers, and shall perform the following:

- Reevaluate whether the person's new duties still require the authority to access CDC's computers.
- Notify the local security coordinator or the access management group if the person no longer requires access authority.
- Notify the owner of the relevant CDC information so that the appropriate paperwork can be initiated to document the removal of the person's access privileges if the person no longer requires access authority.

The lack of use of the access authority is assumed to be proof that the authority is no longer required. Passwords may be revoked without notice if they are not used regularly.

#### **49020.9.1 Annual Information Security Self- Certification**

CDC divisional security coordinators, decentralized end-users, and Local Area Network (LAN) managers are responsible for self-certifying that they are in compliance with applicable CDC information security policies. Responsibility for the dissemination of the policies rests with the owner and the designated security coordinator; responsibility for compliance rests with the end-users.

This policy is intended to ensure compliance by CDC personnel who have been granted access to CDC information resources.

Each CDC division that owns or has custody of decentralized applications shall develop appropriate control entity procedures. Such procedures are subject to approval and audit by the ISO. The procedures are constrained by the following:

- A separate statement of self-certification shall be completed for each organizational entity, where applicable.
- Each statement of self-certification shall be signed by a representative of the senior management of the organizational entity.
- Each statement of self-certification is to be filed unless otherwise instructed by CDC's ISO.

#### **49020.17 Security Awareness Training Within CDC**

All persons who have access to any CDC information shall be provided security awareness training at the time such access begins, and at least annually thereafter.

Security awareness training falls into the following three categories:

##### **Information Security**

All individuals having access to CDC information shall be made aware of the background, scope and objectives of CDC's information security program and of specific CDC information security policies and procedures that are applicable to the level and type of access granted to the individual.

##### **Organizational Security**

All CDC employees shall also be made aware of the events and activities that constitute threats to the organization for which they work, and of the actions to be taken when confronted by those events or activities.

##### **Systems Development/Maintenance Security**

All ISD development/maintenance employees shall also be made aware of State data processing policy and requirements, specific security problems inherent in CDC's automated environment, the need to adequately address information security in feasibility studies, and methods available to eliminate or reduce the security problems in CDC's automated environment.

In order to ensure that all affected persons are consciously aware of their responsibilities for preserving and protecting CDC information resources, initial and periodic information security training is essential.

Appropriate procedures shall be developed by responsible parties (as defined below) to provide the appropriate types of security awareness training for all persons authorized to access CDC information or resources.

The procedures, which are subject to approval by the CDC ISO, shall include the requirement that each person shall sign a CDC security agreement at the conclusion of each information security

training session. Such agreements shall be filed with the access management group to allow renewal of that person's access privilege.

More specifically:

**Information Security Training—CDC Employees**

For each employee authorized to access CDC information resources, the minimum training shall consist of the employee reading DOM 44010 through 44020.

**Information Security Training—Decentralized End-Users**

Each owner of a decentralized application is responsible for the dissemination of all applicable CDC information security policies to the senior management of each decentralized site. The security awareness training policy is applicable to all decentralized sites.

**Information Security Training—Employees of the Department Using CDC's Dedicated Computers**

CDC's ISO shall coordinate with the responsible management of each of these entities to identify the necessary types of security awareness training.

**49020.19.5 Inmate Access to Computers**

It is recognized that inmates knowledgeable about computers represent a valuable resource to the facilities. It is also recognized that a serious risk is created by allowing such inmates to create programs that are used within facilities to support facility work. The purpose of this policy is to minimize the risk involved.

Inmates residing in CDC facilities may have access to microcomputers. This access shall be for the purpose of using a specific computer program or for the purpose of creating a specific computer program. These approved uses of a microcomputer by inmates shall be carried out only under very tightly controlled circumstances.

It is the Department's goal to minimize, and monitor, the use of inmates as programmers for applications used by the Department. To help maintain system security and minimize potential risks, the following procedures shall be followed when utilizing inmates to perform data entry or develop personal computer-based applications:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Computers designated for use by inmate programmers shall not be used concurrently for any other purpose.
- The site's ISC shall approve or disapprove the movement of computers from an "inmate use" status to other work and vice versa.
- Inmates with a work assignment involving a particular computer shall not be assigned to work on other computers.
- Areas where inmates are authorized to work on computers shall be posted as such.
- All inmate computer program development shall be under the supervision of a knowledgeable employee within a controlled, designated area.
- There shall be no communications capabilities in the designated area, such as a telephone line, computer line, telephone punch panel, or radio communication device.

- All inmate-developed programs shall be written in dBase, Foxbase, or Clipper. Existing programs shall be converted to one of these languages.
- Inmates shall not have access to utility programs such as Mace, PCTools, Norton Utilities, Backers Dozen, Take Charge, or any other like software package.
- Inmates shall not have diskettes or any other electronic storage media in their possession except within an approved area.
- Inmates shall not have access to the DOS commands DEBUG, ASSIGN, and ATTRIB.
- Inmates shall not be allowed to load software onto hard disks.
- Source code and documentation shall be reviewed by the AISA prior to final compiling.
- No inmate shall have access to any telecommunication capability.
- No inmate shall have a computer as part of their personal property.
- No inmate shall have a computer in their possession outside of the inmate's authorized work, vocational, or educational areas.



**Attachment B**

**DSE Security Plan**  
*(Separate Document)*